JOINT SOLUTION

Corelight for CrowdStrike Falcon® Exposure Management

ACCELERATE VULNERABILITY DETECTION AND REMEDIATION

By most accounts, SIEMs have succeeded in standardizing and correlating data from different enterprise toolsets. But operationalizing the data to identify and prioritize alerts remains a challenge, giving adversaries the opportunity to dwell on networks for long periods before discovery, and putting organizations at increased risk.

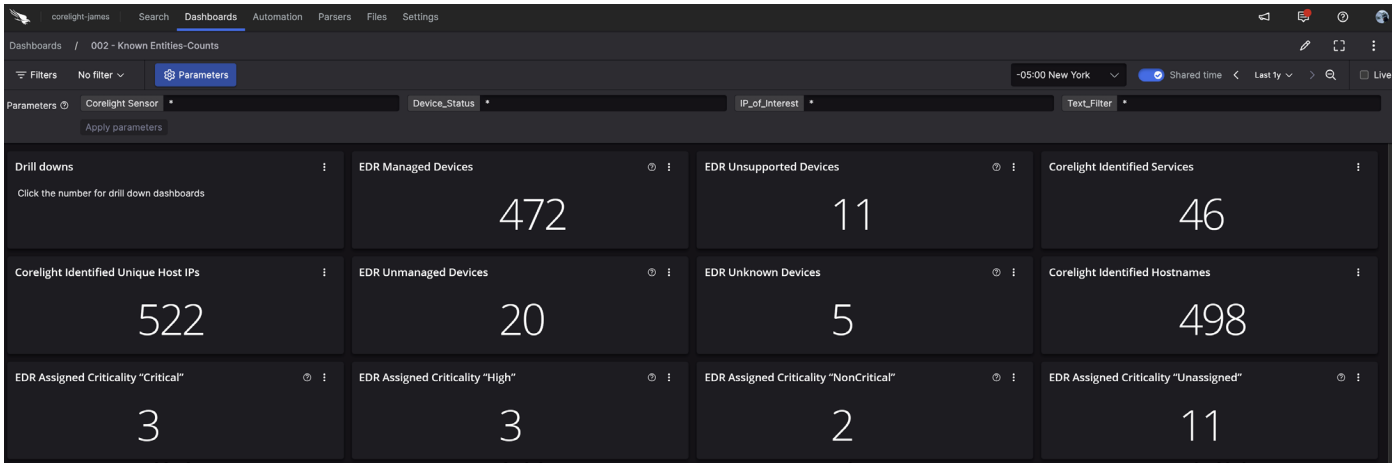
Corelight's Open NDR integration with CrowdStrike Falcon Spotlight, Falcon Discover, Falcon Insight XDR, and Falcon Intelligence addresses this by enriching network telemetry with contextual endpoint data and threat intelligence that can greatly reduce dwell time and simplify exposure management.

In addition to providing rich, contextual evidence of everything traversing the network, Corelight's Open NDR Platform efficiently ingests and enriches network data using information from the Falcon portfolio, such as vulnerability data, threat intelligence, and endpoint information. This contextual insight helps SOC teams identify and prioritize potential exploits that need to be addressed.

INTEGRATION HIGHLIGHTS

- Network logs enriched with contextual endpoint data, vulnerability data, and threat intel
- Integrated data and dashboards simplify and optimize exposure management
- Advanced network telemetry to improve SOC efficiency with risk-based triage and response

INTEGRATION WITH FALCON EXPOSURE MANAGEMENT ACCELERATES DETECTION AND RESPONSE



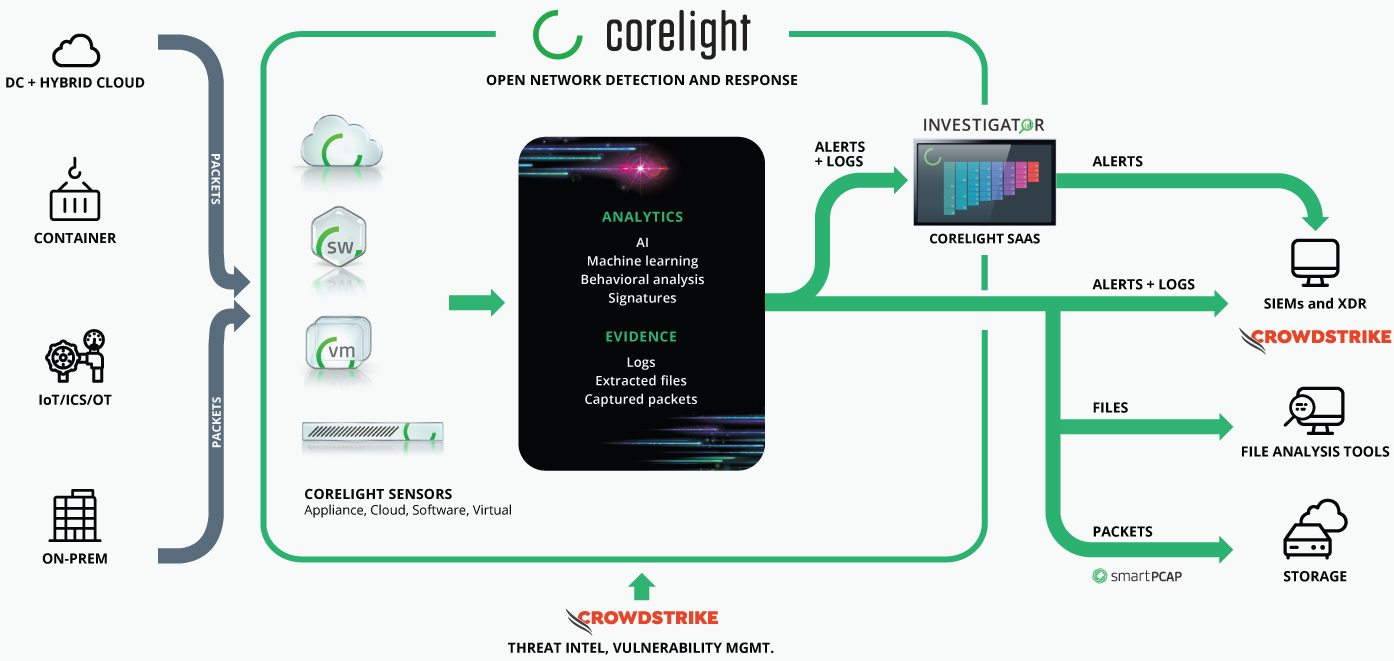
This dashboard highlights CrowdStrike Falcon EDR data enriching Corelight NDR data to provide complete coverage of enterprise devices, ranging from management status of hosts to criticality.

ADVANCED NETWORK TELEMETRY FOR CROWDSTRIKE FALCON

Corelight's Open NDR Platform transforms raw network traffic into comprehensive, evidence to help data-first organizations optimize threat investigations and detections. Native integration across the Falcon portfolio helps resource-constrained Security Operations Center (SOC) teams identify, categorize, and prioritize vulnerabilities across their environment. By ingesting and enriching relevant network logs with endpoint data and threat intelligence through passive network monitoring, Corelight enables Falcon users simplify and optimize their exposure management program.

Knowing where vulnerabilities exist and their relationships to other systems and devices across the network is essential in understanding the organization's holistic risk profile. The real-time, prioritized view of exposures and their related risks across the business can greatly assist security analysts by enabling them to close vulnerabilities more quickly and easily, ensuring they stay one step ahead of adversaries.

CORELIGHT OPEN NDR AND CROWDSTRIKE FALCON EXPOSURE MANAGEMENT



SOLUTION BENEFITS

COMPLETE VISIBILITY

As an inaugural member of CrowdStrike's XDR Alliance program, Corelight enables CrowdStrike customers to optimize exposure management by constantly monitoring and correlating network activity with relevant threat intelligence and endpoint vulnerability data from CrowdStrike Falcon.

NEXT-LEVEL ANALYTICS

Corelight supercharges CrowdStrike Falcon Exposure Management by detecting threats and identifying vulnerabilities before they are exploited. Additionally, Corelight network evidence can detect suspicious activity after adversary initial access, such as data exfiltration, lateral movement, and command and control.

FASTER INVESTIGATION

By correlating alerts, evidence, and packet data, Corelight establishes a network baseline and stores years' worth of activity so analysts can trace the origins of attacks. Contextual evidence integrates directly into CrowdStrike dashboards and workflows to simplify and accelerate investigations.

EXPERT HUNTING

Corelight's integration with CrowdStrike Falcon Exposure Management, Insight XDR, and Threat Intelligence gives SOC teams the insight they need to remediate vulnerabilities faster and easier than ever before. Superior insight and advanced threat detection across the enterprise turns even junior analysts into expert threat hunters.

To learn more about the CrowdStrike integration, request a demo at **https://corelight.com/contact**

CrowdStrike, a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity, and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response Platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497